AUDIT REPORT

Hostname: Access_SW2
Config file name: Access_SW2_startup-config.cfg
Config hash: 29fe36a512321cd0a06027afffe53daf2676fcc4
Vendor: cisco
OS: ios
Facility layer: access
L3 protocols: ipv4
Date: 18/05/2020_09:43

SUCCESS STATISTICS

Weighted score coefficient:	55 out of 100
Successful checks:	34.2%
Unsuccessful checks:	65.8%
Total number of relevant started checks:	149
Successful checks:	51
Unsuccessful 'Critical':	19
Unsuccessful 'High':	42
Unsuccessful 'Medium':	31
Unsuccessful 'Low':	6
Unsuccessful 'Notice':	0

Authentication, Authorization, Accounting

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	AAA new model/ Enabled AAA	High	False	False	Error ✘

Generated fix:
aaa new-model

| 2 | AAA server set | High | False | False | Error ✘ |

Generated fix:
radius server RADIUS_SERVER
address ipv4 192.168.60.11
key RadKey1

| 3 | AAA server group | High | False | False | Error ✘ |

Generated fix:
aaa group server radius RADIUS_SERVER
server name RADIUS_SERVER

| 4 | AAA authentication login | High | False | False | Error ✘ |

Generated fix:
aaa authentication login default group RADIUS_SERVER local enable

| 5 | AAA authentication login fallback | High | False | False | Error ✘ |

Generated fix:
aaa authentication login default group RADIUS_SERVER local enable

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
6	AAA authentication login only local disabled	High	False	False	Successful ✔
7	AAA authentication login none disabled	Critical	False	False	Successful ✔
8	AAA authentication "enable"	Medium	False	False	Error ✘

Generated fix:
aaa authentication enable default group RADIUS_SERVER enable

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
9	AAA authentication "enable" fallback	Medium	False	False	Error ✘

Generated fix:
aaa authentication enable default group RADIUS_SERVER enable

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
10	AAA authentication "enable" only local disabled	Medium	False	False	Successful ✔
11	AAA authentication "enable" none disabled	High	False	False	Successful ✔
12	AAA authorization "exec"	High	False	False	Error ✘

Generated fix:
aaa authorization exec default group RADIUS_SERVER local if-authenticated

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
13	AAA authorization "exec" fallback	High	False	False	Error ✘

Generated fix:
aaa authorization exec default group RADIUS_SERVER local if-authenticated

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
14	AAA authorization "exec" only local disabled	High	False	False	Successful ✔
15	AAA authorization "exec" none disabled	Critical	False	False	Successful ✔
16	AAA accounting "connection"	High	False	False	Error ✘

Generated fix:
aaa accounting connection default start-stop group RADIUS_SERVER

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
17	AAA auccounting "connection" none disabled	High	False	False	Successful ✔
18	AAA accounting "exec"	High	False	False	Error ✘

Generated fix:
aaa accounting exec default start-stop group RADIUS_SERVER

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
19	AAA accounting "exec" none disabled	High	False	False	Successful ✔
20	AAA source interface	Medium	False	False	Error ✘

Generated fix:
ip radius source-interface Loopback0

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
21	AAA authentication max attempts less or equal to 5	High	False	False	Successful ✔

Access to device

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Exec timeout <=5 minutes	Medium	False	False	Error ✘

Found error in context(s):
line con 0
line vty 0 4

Generated fix:
line con 0
exec-timeout 5

line vty 0 4
exec-timeout 5

2	AUX connection input disabled	High	False	False	Successful ✔
3	AUX no execution set	High	False	False	Error ✘

Found error in context(s):
line aux 0

Generated fix:
line aux 0
no exec

4	Remote output connections disabled	Medium	False	False	Error ✘

Found error in context(s):
line con 0
line aux 0
line vty 0 4

Generated fix:
line con 0
transport output none

line aux 0
transport output none

line vty 0 4
transport output none

5	Local user database with encrypted password	Critical	False	False	Error ✘

Generated fix:
username admin secret admin_password

6	Local user database with plaintext password disabled	Critical	False	False	Successful ✔
7	Enable password encrypted	Critical	False	False	Error ✘

Generated fix:
enable secret enablepasswd123

8	Enable password plaintext disabled	Critical	False	False	Successful ✔
9	Local login to virtual terminal disabled	Critical	False	False	Error ✘

Error configuration setting found in:
line vty 0 4
login

Found error in context(s):
line vty 0 4

10	Restrict login to device - IPv4 ACL	Critical	False	False	Error ✘

Found error in context(s):
line vty 0 4

Generated fix:
line vty 0 4
access-class IPV4_VTY_ACL in

11	ACL specified for VTY access is created	Critical	False	False	Error ✘

Comment:
Cannot be fixed automatically!

Fix notice:
Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:
ip access-list standard <acl name>
remark Permiting managemnt device
permit <ip address> <wildcard mask>

12	Log login to device on failure	High	False	False	Error ✘

Generated fix:
login on-failure trap
login on-failure log
login on-failure log-input

Fix notice:
Depending on IOS, usually just one of fixing command is applicable to device. There are more because of different syntax and support among IOS versions.

13	Log login to device on success	Medium	False	False	Error ✘

Generated fix:
login on-success trap
login on-success log
login on-success log-input

Fix notice:
Depending on IOS, usually just one of fixing command is applicable to device. There are more because of different syntax and support among IOS versions.

14	Login quiet mode	Medium	False	False	Error ✘

Generated fix:
login quiet-mode access-class IPV4_VTY_ACL

15	ACL exists for specified login quiet mode	Medium	False	False	Error ✘

Comment:
Cannot be fixed automatically!

Fix notice:
Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for managing devices with these commands:
ip access-list standard <acl name>
remark Permiting managemnt device
permit <ip address> <wildcard mask>

16	One user change config at time	High	False	False	Error ✘

Generated fix:
configuration mode exclusive
configuration mode exclusive auto

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

17	Legal banner MOTD	Low	False	False	Error ✘

Generated fix:
banner motd ; Unauthorized access will be prosecuted!! ;

18	Legal banner exec	Low	False	False	Error ✘

Generated fix:
banner exec ; Unauthorized access will be prosecuted!! ;

19	Legal banner login	Low	False	False	Error ✘

Generated fix:
banner login ; Unauthorized access will be prosecuted!! ;

20	Session timeout	Medium	False	False	Error ✘

Found error in context(s):
line con 0
line aux 0
line vty 0 4

Generated fix:
line con 0
session-timeout 30

line aux 0
session-timeout 30

line vty 0 4
session-timeout 30

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
21	AUX exec timeout one second	High	False	False	Error ✘

Found error in context(s):
line aux 0

Generated fix:
line aux 0
exec-timeout 0 1

| 22 | Restrict login to device - IPv6 ACL | Critical | True | False | Not relevant ✔ |

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

| 23 | ACL IPv6 specified for VTY access is created | Critical | True | False | Not relevant ✔ |

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

| 24 | Login DOS block for | High | False | False | Error ✘ |

Generated fix:
login block-for 120 attempts 3 within 30

SSH

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	SSH enable on management connection	Critical	False	False	Error ✘

Found error in context(s):
line vty 0 4

Generated fix:
line vty 0 4
transport input ssh

Fix notice:
Make sure RSA key is present - generated or imported. For generating RSA key, issue command:
crypto key generate rsa modulus 2048

| 2 | SSH version 2 | Critical | False | False | Error ✘ |

Generated fix:
ip ssh version 2

| 3 | SSH timeout | Medium | False | False | Error ✘ |

Generated fix:
ip ssh timeout 30
ip ssh time-out 30

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
4	SSH max 3 retries	Medium	False	False	Successful ✔
5	SSH source interface	High	False	False	Error ✘

Generated fix:
ip ssh source-interface Loopback0

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
6	SSH not default port	High	False	False	Error ✘

Generated fix:
ip ssh port 2223 rotary 1

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
7	SSH not default port applied	High	False	False	Error ✘

Found error in context(s):
line vty 0 4

Generated fix:
line vty 0 4
rotary 1

Device identification

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Hostname set	Low	False	False	Successful ✔

Comment:
Cannot be fixed automatically!

Right configuration setting found in:
hostname Access_SW2

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
2	Domain name set	Low	False	False	Error ✘

Generated fix:
ip domain-name thesis-test.cz
ip domain name thesis-test.cz

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
3	All interfaces have description	Low	False	False	Error ✘

Comment:
Cannot be fixed automatically!

Right configuration setting found in:
interface Ethernet0/0
description trusted-uplink
interface Ethernet0/1
description trusted-uplink

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3
Serial4/0
Serial4/1
Serial4/2
Serial4/3
Serial5/0
Serial5/1
Serial5/2
Serial5/3
Vlan1

Fix notice:
Set interface descrtiption with command:
interface <interface name>
description <description of interface>

Fix ignore comment:
Fixing commands suppressed due to manual need of manual chenage and name determination.

SNMP

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	SNMP v2 write disabled	Critical	False	False	Successful ✔
2	SNMP v2 read without ACL disabled	Critical	False	False	Successful ✔
3	SNMP v2 read with ACL disabled	Critical	False	False	Successful ✔
4	SNMP v1 trap host disabled	Critical	False	False	Successful ✔
5	SNMP v2 trap host disabled	Critical	False	False	Successful ✔
6	SNMP v3 read [authnopriv|noauth|authpriv without ACL] or write disabled	Critical	False	False	Successful ✔
7	SNMP v3 read authpriv with ACL enabled	Critical	False	False	Error ✘

Generated fix:
snmp-server group SNMP_V3_GRP v3 priv read READVIEWv3 access SNMP_V3
snmp-server user SNMPv3USER SNMP_V3_GRP v3 auth sha SnmpPasswd123 priv aes 256 SnmpPasswd123 access SNMP_V3

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
8	SNMP v3 read authpriv with IPv6 ACL enabled	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
9	SNMP user v1|v2c or v3 [noauth|authnopriv|no sha|no aes|without ACL] disabled	Critical	False	False	Successful ✔
10	SNMP trap source interface	High	False	False	Error ✘

Generated fix:
snmp-server trap-source Loopback0

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
11	SNMP server location	High	False	False	Error ✘

Generated fix:
snmp-server location GNS3LAB

12	SNMP v3 traps priv	Medium	False	False	Error ✘

Generated fix:
snmp-server host 192.168.60.11 version 3 priv SNMPv3USER

13	SNMP traps v3 read [authnopriv|noauth] or v1|v2 disabled	Critical	False	False	Successful ✔
14	SNMP traps enabled	Medium	False	False	Error ✘

Generated fix:
snmp-server enable traps

15	ACL is created for SNMPv3	Critical	False	False	Error ✘

Comment:
Cannot be fixed automatically!

Fix notice:
Cannot be fixed automatically! If search is not successful create ACL, which permits only needed end stations for receiving SNMP with these commands:
ip access-list standard <acl name>
remark Permiting SNMP
permit <ip address> <wildcard mask>

16	ACL IPv6 is created for SNMPv3	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

17	SNMP interface index persist enabled globally	High	False	False	Error ✘

Generated fix:
snmp-server ifindex persist
snmp ifmib ifindex persist

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

18	SNMP interface index persist enabled per interface	High	False	False	Error ✘

Found port(s) with error:
Ethernet0/0
Ethernet0/1
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3
Serial4/0
Serial4/1
Serial4/2
Serial4/3
Serial5/0
Serial5/1
Serial5/2
Serial5/3
Vlan1

Generated fix:
interface Ethernet0/0
snmp ifindex persist
exit
interface Ethernet0/1
snmp ifindex persist
exit
interface Ethernet0/2
snmp ifindex persist
exit
interface Ethernet0/3
snmp ifindex persist
exit
interface Ethernet1/0
snmp ifindex persist
exit
interface Ethernet1/1
snmp ifindex persist
exit
interface Ethernet1/2
snmp ifindex persist
exit
interface Ethernet1/3
snmp ifindex persist
exit
interface Ethernet2/0
snmp ifindex persist
exit
interface Ethernet2/1
snmp ifindex persist
exit
interface Ethernet2/2
snmp ifindex persist
exit
interface Ethernet2/3
snmp ifindex persist
exit
interface Ethernet3/0
snmp ifindex persist
exit
interface Ethernet3/1
snmp ifindex persist
exit
interface Ethernet3/2
snmp ifindex persist
exit
interface Ethernet3/3
snmp ifindex persist
exit
interface Serial4/0
snmp ifindex persist
exit
interface Serial4/1
snmp ifindex persist
exit
interface Serial4/2
snmp ifindex persist
exit
interface Serial4/3
snmp ifindex persist
exit
interface Serial5/0
snmp ifindex persist
exit
interface Serial5/1
snmp ifindex persist
exit
interface Serial5/2
snmp ifindex persist
exit
interface Serial5/3
snmp ifindex persist
exit
interface Vlan1
snmp ifindex persist
exit

Syslog

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Syslog server enabled	High	False	False	Error ✘

Generated fix:
logging host 192.168.60.11

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
2	Syslog server IPv6 enabled	High	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
3	Syslog source interface	Medium	False	False	Error ✘

Generated fix:
logging source-interface Loopback0

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
4	Syslog format	Medium	False	False	Successful ✔

Right configuration setting found in:
service timestamps log datetime msec

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
5	Syslog critical alerts to console	Medium	False	False	Error ✘

Generated fix:
logging console critical

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
6	Syslog send informational traps	High	False	False	Successful ✔
7	Syslog buffer set with severity	High	False	False	Error ✘

Generated fix:
logging buffered 40960 informational

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
8	Syslog local backup	High	False	False	Error ✘

Generated fix:
logging persistent url flash:

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
9	Syslog sequence numbers added	Medium	False	False	Error ✘

Generated fix:
service sequence-numbers

NTP

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	NTP server set	High	False	False	Error ✘

Generated fix:
ntp server 192.168.60.11

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
2	NTP source interface	Medium	False	False	Error ✘

Generated fix:
ntp source Loopback0

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
3	NTP authentication key	High	False	False	Error ✘

Generated fix:
ntp authentication-key 1 md5 ntpPasswd123

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
4	NTP trusted key	High	False	False	Error ✘

Generated fix:
ntp trusted-key 1

| 5 | NTP authenticate | High | False | False | Error ✘ |

Generated fix:
ntp authenticate

High load

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	SNMP traps for CPU load	Medium	False	False	Error ✘

Generated fix:
snmp-server enable traps cpu threshold

| 2 | Threshold for CPU load | Medium | False | False | Error ✘ |

Generated fix:
process cpu threshold type total rising 70 interval 5

| 3 | Statistics entry for CPU load | Low | False | False | Error ✘ |

Generated fix:
process cpu statistics limit entry-percentage 70

| 4 | Reserve memory for critical notification | Medium | False | False | Error ✘ |

Generated fix:
memory reserve critical 1000

| 5 | Minimum CPU memory notification | Medium | False | False | Error ✘ |

Generated fix:
memory free low-watermark processor 2000

| 6 | Minimum IO memory notification | Medium | False | False | Error ✘ |

Generated fix:
memory free low-watermark io 2000

Spanning tree

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Portfast globally enabled	High	False	False	Error ✘

Generated fix:
spanning-tree portfast default
spanning-tree portfast edge default

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

| 2 | Portfast enabled on access interface | High | False | False | Error ✘ |

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/2
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet0/3
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet1/0
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet1/1
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet1/2
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet1/3
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet2/0
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet2/1
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet2/2
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet2/3
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet3/0
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet3/1
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet3/2
spanning-tree portfast
spanning-tree portfast edge
exit
interface Ethernet3/3
spanning-tree portfast
spanning-tree portfast edge
exit

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

3	BPDU Guard globally enabled	Critical	False	False	Error ✗

Generated fix:
spanning-tree portfast bpduguard default
spanning-tree portfast edge bpduguard default

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

4	BPDU Guard enabled on access interface	High	False	False	Error ✘

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/2
spanning-tree bpduguard enable
exit
interface Ethernet0/3
spanning-tree bpduguard enable
exit
interface Ethernet1/0
spanning-tree bpduguard enable
exit
interface Ethernet1/1
spanning-tree bpduguard enable
exit
interface Ethernet1/2
spanning-tree bpduguard enable
exit
interface Ethernet1/3
spanning-tree bpduguard enable
exit
interface Ethernet2/0
spanning-tree bpduguard enable
exit
interface Ethernet2/1
spanning-tree bpduguard enable
exit
interface Ethernet2/2
spanning-tree bpduguard enable
exit
interface Ethernet2/3
spanning-tree bpduguard enable
exit
interface Ethernet3/0
spanning-tree bpduguard enable
exit
interface Ethernet3/1
spanning-tree bpduguard enable
exit
interface Ethernet3/2
spanning-tree bpduguard enable
exit
interface Ethernet3/3
spanning-tree bpduguard enable
exit

5	BPDU Filter globally disabled	Critical	False	False	Successful ✔

6	BPDU Filter disabled on access interface	High	False	False	Not relevant ✔

Comment:
Module 09_06_stp_bpdu_filter_interface.yaml configured to run after 09_05_stp_bpdu_filter.yaml with status error but that module has not run yet with specified cmd_match_status, 09_06_stp_bpdu_filter_interface.yaml will not run

7	Loop Guard globally enabled	Critical	False	False	Error ✘

Generated fix:
spanning-tree loopguard default

8	Loop Guard enabled on access interface	High	False	False	Error ✘

Found port(s) with error:
Ethernet0/0
Ethernet0/1
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/0
spanning-tree guard loop
exit
interface Ethernet0/1
spanning-tree guard loop
exit
interface Ethernet0/2
spanning-tree guard loop
exit
interface Ethernet0/3
spanning-tree guard loop
exit
interface Ethernet1/0
spanning-tree guard loop
exit
interface Ethernet1/1
spanning-tree guard loop
exit
interface Ethernet1/2
spanning-tree guard loop
exit
interface Ethernet1/3
spanning-tree guard loop
exit
interface Ethernet2/0
spanning-tree guard loop
exit
interface Ethernet2/1
spanning-tree guard loop
exit
interface Ethernet2/2
spanning-tree guard loop
exit
interface Ethernet2/3
spanning-tree guard loop
exit
interface Ethernet3/0
spanning-tree guard loop
exit
interface Ethernet3/1
spanning-tree guard loop
exit
interface Ethernet3/2
spanning-tree guard loop
exit
interface Ethernet3/3
spanning-tree guard loop
exit

VLAN

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Default Vlan not used	Critical	False	False	Error ✘

Comment:
Cannot be fixed automatically! Cannot automatically determine VLAN assignment to port.

Right configuration setting found in:
interface Ethernet0/2
switchport access vlan 30

Found port(s) with error:
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Fix notice:
Eliminate ports with default Vlan by command with Vlan ID different than 1
interface <interface name>
switchport mode access
switchport access vlan <vlan id>

2	Management VLAN + SVI set and different than 1	Medium	False	False	Error ✘

Comment:
Cannot be fixed automatically! Cannot automatically set diffrenet IP among SVI(s) a lot of prerequirements must be met as existing VLAN and port assigned to VLAN.

Fix notice:
If successful, it means SVI was found, but it might not be management VLAN!! Management VLAN can be created with command:
interface Vlan <vlan id>
ip address <ip> <mask>
no shutdown

3	Management VLAN gateway	Medium	False	False	Successful ✔

Comment:
Cannot be fixed automatically! Cannot automatically set default gateway among different switches.

Right configuration setting found in:
ip default-gateway 192.168.30.1

4	Native vlan different than 1	Critical	False	False	Successful ✔

Right configuration setting found in:
interface Ethernet0/0
switchport trunk native vlan 100
interface Ethernet0/1
switchport trunk native vlan 100

5	Specified allowed VLAN on trunk	Critical	False	False	Successful ✔

Right configuration setting found in:
interface Ethernet0/0
switchport trunk allowed vlan 20,30
interface Ethernet0/1
switchport trunk allowed vlan 20,30

6	Switchport mode dynamic disabled	Critical	False	False	Successful ✔
7	Switchport implicit dynamic disabled	Critical	False	False	Error ✘

Right configuration setting found in:
interface Ethernet0/2
switchport mode access

Found port(s) with error:
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/3
switchport mode access
exit
interface Ethernet1/0
switchport mode access
exit
interface Ethernet1/1
switchport mode access
exit
interface Ethernet1/2
switchport mode access
exit
interface Ethernet1/3
switchport mode access
exit
interface Ethernet2/0
switchport mode access
exit
interface Ethernet2/1
switchport mode access
exit
interface Ethernet2/2
switchport mode access
exit
interface Ethernet2/3
switchport mode access
exit
interface Ethernet3/0
switchport mode access
exit
interface Ethernet3/1
switchport mode access
exit
interface Ethernet3/2
switchport mode access
exit
interface Ethernet3/3
switchport mode access
exit

8	DTP disabled	Critical	False	False	Error ✘

Right configuration setting found in:
interface Ethernet0/0
switchport nonegotiate
interface Ethernet0/1
switchport nonegotiate

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/2
switchport nonegotiate
exit
interface Ethernet0/3
switchport nonegotiate
exit
interface Ethernet1/0
switchport nonegotiate
exit
interface Ethernet1/1
switchport nonegotiate
exit
interface Ethernet1/2
switchport nonegotiate
exit
interface Ethernet1/3
switchport nonegotiate
exit
interface Ethernet2/0
switchport nonegotiate
exit
interface Ethernet2/1
switchport nonegotiate
exit
interface Ethernet2/2
switchport nonegotiate
exit
interface Ethernet2/3
switchport nonegotiate
exit
interface Ethernet3/0
switchport nonegotiate
exit
interface Ethernet3/1
switchport nonegotiate
exit
interface Ethernet3/2
switchport nonegotiate
exit
interface Ethernet3/3
switchport nonegotiate
exit

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
9	VTP disabled	Critical	False	False	Successful ✔

Network Mapping

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	CDP globally disabled	Critical	False	False	Error ✘

Generated fix:
no cdp run

Fix notice:
Services such as Cisco IP telephony would not work

| 2 | CDP disabled on interface(s) | Critical | False | False | Error ✘ |

Found port(s) with error:
Ethernet0/0
Ethernet0/1
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3
Serial4/0
Serial4/1
Serial4/2
Serial4/3
Serial5/0
Serial5/1
Serial5/2
Serial5/3

Generated fix:
interface Ethernet0/0
no cdp enable
exit
interface Ethernet0/1
no cdp enable
exit
interface Ethernet0/2
no cdp enable
exit
interface Ethernet0/3
no cdp enable
exit
interface Ethernet1/0
no cdp enable
exit
interface Ethernet1/1
no cdp enable
exit
interface Ethernet1/2
no cdp enable
exit
interface Ethernet1/3
no cdp enable
exit
interface Ethernet2/0
no cdp enable
exit
interface Ethernet2/1
no cdp enable
exit
interface Ethernet2/2
no cdp enable
exit
interface Ethernet2/3
no cdp enable
exit
interface Ethernet3/0
no cdp enable
exit
interface Ethernet3/1
no cdp enable
exit
interface Ethernet3/2
no cdp enable
exit
interface Ethernet3/3
no cdp enable
exit
interface Serial4/0
no cdp enable
exit
interface Serial4/1
no cdp enable
exit
interface Serial4/2
no cdp enable
exit
interface Serial4/3
no cdp enable
exit
interface Serial5/0
no cdp enable
exit
interface Serial5/1
no cdp enable
exit
interface Serial5/2
no cdp enable
exit
interface Serial5/3
no cdp enable
exit

| 3 | LLDP globally disabled | Critical | False | False | Successful ✔ |
| 4 | LLDP receive disabled on interface(s) | Critical | False | False | Not relevant ✔ |

Comment:
Module 11_04_lldp_receive.yaml configured to run after 11_03_lldp_run_disabled.yaml with status error but that module has not run yet with specified cmd_match_status, 11_04_lldp_receive.yaml will not run

5	LLDP transmit disabled on interface(s)	Critical	False	False	Not relevant ✔

Comment:
Module 11_05_lldp_transmit.yaml configured to run after 11_03_lldp_run_disabled.yaml with status error but that module has not run yet with specified cmd_match_status, 11_05_lldp_transmit.yaml will not run

6	ICMP 224.0.0.1 ping disabled in ACL	Medium	False	False	Error ✘

Generated fix:
ip access-list extended DENY_NETWORK_MAP
remark deny ping all nodes
deny icmp any host 224.0.0.1 echo log-input
remark deny host query
deny igmp any any host-query log-input
permit ip any any

Fix notice:
Some devices do not recognize parameter "log-input" in ACL, so manually replace it with "log"

7	IGMP Host Query disabled in ACL	Medium	False	False	Error ✘

Generated fix:
ip access-list extended DENY_NETWORK_MAP
remark deny ping all nodes
deny icmp any host 224.0.0.1 echo log-input
remark deny host query
deny igmp any any host-query log-input
permit ip any any

Fix notice:
Some devices do not recognize parameter "log-input" in ACL, so manually replace it with "log"

8	ICMPv6 ff02::1 ping disabled in ACL	Medium	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

9	MLD Host Query disabled in ACL	Medium	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

10	ACL against IPv4 network monitoring applied on interface(s)	Medium	False	False	Error ✘

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/2
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet0/3
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet1/0
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet1/1
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet1/2
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet1/3
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet2/0
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet2/1
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet2/2
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet2/3
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet3/0
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet3/1
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet3/2
ip access-group DENY_NETWORK_MAP in
exit
interface Ethernet3/3
ip access-group DENY_NETWORK_MAP in
exit

Fix notice:
ACL will be applied to specified ACCESS interface(s). In case of existing ACL on interface in same direction, please set variable fix_cmd_ignore: "true" and append generated ACL from module 11_12_icmp_discovery_network to existing ACL to proper place.

| 11 | ACL against IPv6 network monitoring applied on interface(s) | Medium | True | False | Not relevant ✔ |

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

Filtering

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	ACL filter IPv6 unknown extended header	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

| 2 | ACL filter IPv6 unknown extended header applied on ACCESS interface | Critical | True | False | Not relevant ✔ |

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

First Hop Security

No.	Name	Severity	Skipped	Cannot determine search/fix	Status

| 1 | Port security enabled | Critical | False | False | Error ✖ |

Right configuration setting found in:
interface Ethernet0/2
switchport port-security

Found port(s) with error:
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/3
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet1/0
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet1/1
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet1/2
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet1/3
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet2/0
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet2/1
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet2/2
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet2/3
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet3/0
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet3/1
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet3/2
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit
interface Ethernet3/3
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
switchport port-security
exit

2	Port security maximum 1 allowed MAC on port	Critical	False	False	Successful ✔

3	Port security violation shutdown	Critical	False	False	Successful ✔
4	802.1x globally enabled	High	False	False	Error ✘

Generated fix:
dot1x system-auth-control

5	AAA authentication 802.1x	High	False	False	Error ✘

Generated fix:
aaa authentication dot1x default group RADIUS_SERVER

6	802.1x enabled on interfaces	High	False	False	Error ✘

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/2
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet0/3
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet1/0
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet1/1
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet1/2
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet1/3
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet2/0
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet2/1
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet2/2
access-session port-control auto

```
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet2/3
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet3/0
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet3/1
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet3/2
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
interface Ethernet3/3
access-session port-control auto
authentication port-control auto
dot1x port-control auto
yes
exit
```

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

7	802.1x enabled on interfaces	High	False	False	Successful ✔
8	802.1x port set authenticator	High	False	False	Error ✘

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/2
dot1x pae authenticator
exit
interface Ethernet0/3
dot1x pae authenticator
exit
interface Ethernet1/0
dot1x pae authenticator
exit
interface Ethernet1/1
dot1x pae authenticator
exit
interface Ethernet1/2
dot1x pae authenticator
exit
interface Ethernet1/3
dot1x pae authenticator
exit
interface Ethernet2/0
dot1x pae authenticator
exit
interface Ethernet2/1
dot1x pae authenticator
exit
interface Ethernet2/2
dot1x pae authenticator
exit
interface Ethernet2/3
dot1x pae authenticator
exit
interface Ethernet3/0
dot1x pae authenticator
exit
interface Ethernet3/1
dot1x pae authenticator
exit
interface Ethernet3/2
dot1x pae authenticator
exit
interface Ethernet3/3
dot1x pae authenticator
exit

9	DHCP Snooping globally enabled	Critical	False	False	Error ✘

Generated fix:
ip dhcp snooping

Fix notice:
On router(s) to DHCP server issue command "ip dhcp relay information trust-all"

10	DHCP Snooping enabled for VLAN(s)	Critical	False	False	Successful ✔

Right configuration setting found in:
ip dhcp snooping vlan 1,20,30,100

11	DHCP Snooping trust interface(s) set	Critical	False	False	Successful ✔

Right configuration setting found in:
interface Ethernet0/0
ip dhcp snooping trust
interface Ethernet0/1
ip dhcp snooping trust

12	DHCP Snooping rate limit fo ACCESS interface(s) set	High	False	False	Error ✘

Found port(s) with error:
Ethernet0/2
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/2
ip dhcp snooping limit rate 100
exit
interface Ethernet0/3
ip dhcp snooping limit rate 100
exit
interface Ethernet1/0
ip dhcp snooping limit rate 100
exit
interface Ethernet1/1
ip dhcp snooping limit rate 100
exit
interface Ethernet1/2
ip dhcp snooping limit rate 100
exit
interface Ethernet1/3
ip dhcp snooping limit rate 100
exit
interface Ethernet2/0
ip dhcp snooping limit rate 100
exit
interface Ethernet2/1
ip dhcp snooping limit rate 100
exit
interface Ethernet2/2
ip dhcp snooping limit rate 100
exit
interface Ethernet2/3
ip dhcp snooping limit rate 100
exit
interface Ethernet3/0
ip dhcp snooping limit rate 100
exit
interface Ethernet3/1
ip dhcp snooping limit rate 100
exit
interface Ethernet3/2
ip dhcp snooping limit rate 100
exit
interface Ethernet3/3
ip dhcp snooping limit rate 100
exit

13	IPv6 Unicast Routing enabled	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

14	IPv6 RA Guard host policy defined	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

15	IPv6 RA Guard on ACCESS interface(s)	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

16	DHCPv6 Server policy	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

17	DHCPv6 Client policy	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

18	DHCPv6 Guard server interface(s) set	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

19	DHCPv6 Guard client interface(s) set	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

20	Dynamic ARP Inspection enabled for VLAN(s)	Critical	False	False	Successful ✔

Right configuration setting found in:
ip arp inspection vlan 20,30

21	Dynamic ARP Inspection validate by SRC,DST MAC and IP	Critical	False	False	Successful ✔

Right configuration setting found in:
ip arp inspection validate src-mac dst-mac ip

22	Dynamic ARP trusted interface(s) set	Critical	False	False	Successful ✔

Right configuration setting found in:
interface Ethernet0/0
ip arp inspection trust
interface Ethernet0/1
ip arp inspection trust

23	IPv6 ND inspection policy	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

24	IPv6 ND inspection on interface(s) set	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

25	IPv6 Snooping policy	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

26	IPv6 Snooping on interface(s) set	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

27	IP Source Guard on interface(s) set	Critical	False	False	Error ✘

Right configuration setting found in:
interface Ethernet0/2
ip verify source port-security

Found port(s) with error:
Ethernet0/3
Ethernet1/0
Ethernet1/1
Ethernet1/2
Ethernet1/3
Ethernet2/0
Ethernet2/1
Ethernet2/2
Ethernet2/3
Ethernet3/0
Ethernet3/1
Ethernet3/2
Ethernet3/3

Generated fix:
interface Ethernet0/3
ip verify source port-security
exit
interface Ethernet1/0
ip verify source port-security
exit
interface Ethernet1/1
ip verify source port-security
exit
interface Ethernet1/2
ip verify source port-security
exit
interface Ethernet1/3
ip verify source port-security
exit
interface Ethernet2/0
ip verify source port-security
exit
interface Ethernet2/1
ip verify source port-security
exit
interface Ethernet2/2
ip verify source port-security
exit
interface Ethernet2/3
ip verify source port-security
exit
interface Ethernet3/0
ip verify source port-security
exit
interface Ethernet3/1
ip verify source port-security
exit
interface Ethernet3/2
ip verify source port-security
exit
interface Ethernet3/3
ip verify source port-security
exit

| 28 | IPv6 Source Guard policy | Critical | True | False | Not relevant ✔ |

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
29	IPv6 Source Guard on interface(s) set	Critical	True	False	Not relevant ✔

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

| 30 | IPv6 Destination Guard policy | Critical | True | False | Not relevant ✔ |

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

| 31 | IPv6 Destination Guard on interface(s) set | Critical | True | False | Not relevant ✔ |

Comment:
Skipped, required function ipv6 not configured on device. Everything is OK.

Other

No.	Name	Severity	Skipped	Cannot determine search/fix	Status
1	Servis PAD disabled (Packet assembler disassembler)	High	False	False	Error ✗

Generated fix:
no service pad

| 2 | BOOTP server disabled | High | False | False | Error ✗ |

Generated fix:
no ip bootp server

3	Finger protocol disabled	High	False	False	Successful ✔
4	HTTP server disabled	High	False	False	Successful ✔
5	HTTPS server disabled	High	False	False	Successful ✔
6	TCP small server disabled	High	False	False	Successful ✔
7	UDP small server disabled	High	False	False	Successful ✔
8	IP domain lookup disabled	High	False	False	Successful ✔

Right configuration setting found in:
no ip domain-lookup

| 9 | Gratuitous ARPs generation disabled | High | False | False | Error ✗ |

Generated fix:
no ip gratuitous-arps

| 10 | Gratuitous ARPs reject enabled | High | False | False | Error ✗ |

Generated fix:
ip arp gratuitous none

| 11 | Netflow is disabled | Notice | False | False | Successful ✔ |

Fix ignore comment:
By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is neccesary for monitoring

| 12 | Netflow version 9 used | Medium | False | False | Not relevant ✔ |

Comment:
Module 15_14_netflow_version_9.yaml configured to run after 15_13_netflow.yaml with status error but that module has not run yet with specified cmd_match_status, 15_14_netflow_version_9.yaml will not run

| 13 | Netflow traffic analyze disabled on interface(s) | Notice | False | False | Not relevant ✔ |

Comment:
Module 15_15_netflow_interface.yaml configured to run after 15_13_netflow.yaml with status error but that module has not run yet with specified cmd_match_status, 15_15_netflow_interface.yaml will not run

Fix ignore comment:
By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is neccesary for monitoring

14	Port mirroring disabled on interface(s)	Notice	False	False	Successful ✔

Fix ignore comment:
By default fix is ignored due to disablement of traffic monitoring. Consider whether port mirroring is neccesary for monitoring

15	Notification on memory IO leak/overflow	Medium	False	False	Error ✘

Generated fix:
exception memory ignore overflow io

16	Notification on memory CPU leak/overflow	Medium	False	False	Error ✘

Generated fix:
exception memory ignore overflow processor

17	Network boot disabled	Medium	False	False	Successful ✔
18	Network config load disabled	Medium	False	False	Successful ✔
19	SCP server enabled	Medium	False	False	Error ✘

Generated fix:
ip scp server enable

20	SCP alias copy instead of TFTP	High	False	False	Successful ✔
21	Protection of configuration deletion	High	False	False	Error ✘

Generated fix:
secure boot config
secure boot-config

Fix notice:
Just one of fixing command is applicable to device. There are more because of different syntax among IOS versions.

22	Archive and log config changes	Medium	False	False	Error ✘

Generated fix:
archive
path unix:
log config
logging enable
notify syslog
hidekeys
maximum 5
time-period 60

23	Terminate hanged inbound TCP connection to device	Medium	False	False	Error ✘

Generated fix:
service tcp-keepalives-in

24	Terminate hanged outbound TCP connection to device	Medium	False	False	Error ✘

Generated fix:
service tcp-keepalives-out

25	Encrypt all saved passwords in configuration	Critical	False	False	Successful ✔

Right configuration setting found in:
no service password-encryption